AMENDMENTS TO THE SPECIFICATION:

Please replace the second paragraph on page 4 with the following amended paragraph:

Exemplary methods of the present invention ~~may~~ enable the debit and credit transactions to be carried out using a cryptographic token, where it is required that the authentication and cryptographic checksum process are performed on the counter content using a challenge/response method. A single challenge/response method can then be applied, whereby only one random number is provided by the security module SM and only one response is calculated by the chip card, to verify both the identity (authentication) as well as the internal counter content with respect to the security module SM.

Please replace the first paragraph on page 5 with the following amended paragraph:

assume that a linear-feedback shift register (LFSR) having an additional nonlinear function and downstream counters is used. Exemplary steps and features ~~may~~ include that:

additional feedback circuits are switched into the linear-feedback shift register LFSR following the downstream counters;

input data, composed of the non-secret card data D and the secret key K, are read into the linear-feedback shift register LFSR, while both the feedback of the linear-feedback shift register LFSR, as well as the additional feedback(s) are active;

a certain number of clock pulses is processed without additional input data being read in;

input data made up of the random number R are read in while both the feedback of the LFSR and the additional feedback(s) are active;

the additional feedback circuits are switched off, and the counters are reset, if necessary; and/or

a certain number of clock pulses, for example, a third number of pulses of the clock, is

processed, and, during these pulses, output bits are generated according to the current counter settings.

Please add the following new paragraph after the first paragraph on page 5:

A further exemplary method for loading input data into a program when performing a cash transaction authentication between and electronic cash chip card and a security module, the chip card including a stored credit balance, involves debiting a requested cash amount from the chip card using a security function. The requested cash amount is added and stored in a cash amount summing counter of the security module. The input data is subdivided into a plurality of data blocks. The plurality of data blocks are loaded into a linear-feedback shift register for performing the program. The linear-feedback shift register has at least one non-linear function cryptographically enhanced using at least one downstream counter. At least one additional feedback is introduced into the linear-feedback shift register following the at least one downstream counter. The at least one additional feedback is switched off after a predefined first number of pulses of an associated clock. The at least one downstream counter and the first number of clock pulses are selected so as to enable calculating an authentication token to be based on a second number of clock pulses.

Please add the following three new paragraphs after the first paragraph (reciting "Fig. 2 shows...") on page 3:

Fig. 3 shows a diagram of another exemplary method and/or embodiment according to the present invention.

Fig. 4 shows a diagram of another exemplary method and/or embodiment according to the present invention.

Fig. 5 shows a diagram of another exemplary method and/or embodiment according to the present invention.

Please add the following three new paragraphs after the first paragraph on page 4:

Fig. 3 shows a diagram of an exemplary device 130 according to the present invention for loading input data into a program when performing an authentication using a cryptographic MAC function. The device 130 shown includes a circuit 140. Circuit 140 includes counter A 132. Counter A is connected to both linear feedback shift register 134 and latch 135. The linear feedback shift register 134 may have a nonlinear feed-forward function for reading off from the linear-feedback shift register 134 and for influencing an output of the linear-feedback shift register 134 using counter A 132. The device 130 further includes at least one counter B 136 for performing a program associated with the present invention. Counter B 136 is connected downstream from the linear-feedback shift register 134. The device further may include at least one non-linear feedback shift register 138 for cryptographically enhancing the device 130, the at least one additional non-linear feedback shift 138 being disconnectable via latch 135 from the device 130. In this exemplary device 130, counter A 132 and/or counter B 136 can may be subdivided or reduced.

Fig. 4 shows a diagram of an exemplary device 130 similar to the device shown in Fig. 3, and including multiple linear-feedback shift registers 134a, 134b (in place of linear-feedback shift register 134) and multiple counters 136a, 136b (in place of counter B 136). Further, Fig. 4 shows feedback from a first downstream counter 136a being provided into the linear feedback shift register 134a. The first downstream counter 136a is arranged before latch 135.

Fig. 5 shows a flow chart of an exemplary method of the present invention. A device for loading input data into a program when performing an authentication using a cryptographic MAC function is provided and includes a first counter 200. A linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register and for influencing an output of the linear feedback shift register using the first counter is provided, the linear-feedback shift register forming at least part of a circuit 202. At least one second counter for performing the program is connected downstream of the linear-feedback shift register 204. An additional non-linear feedback shift register is provided for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable 206. The device further provides a latch 208. And, additional feedback is generated as an XOR sum of readouts

following a first of the at least one second downstream counter before the latch, from the latch following the first of the at least one second downstream counter, and following a second of the at least one second downstream counter 210.